UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,914	01/29/2002	Jens-Peter Redlich	A7995	3714

7590 09/28/2011

SUGHRUE MION, PLLC
2100 Pennsylvania Avenue NW
Washington, DC 20037-3213

EXAMINER	
PATEL, CHIRAG R	
ART UNIT	PAPER NUMBER
2454	
MAIL DATE	DELIVERY MODE
09/28/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JENS-PETER REDLICH, THOMAS KUEHNEL,
and WOLF MUELLER

Appeal 2009-010959
Application 10/057,914
Technology Center 2400

Before HOWARD B. BLANKENSHIP, JOHN A. JEFFERY, and CAROLYN D. THOMAS, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-34 and 36-41, which are all the claims remaining in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Representative Claim

1. A method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A);

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A);

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A);

upon authentication of said terminal (U) and said ISP (P), said ISP performs the following:

generating a session key;

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T);

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T);

wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said untrusted access station (A),

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

Examiner's Rejections

Claims 1-22, 24, 25, 28-32, 36, 37, 39, and 40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Slemmer (US 6,226,677 B1) and Giniger (US 6,751,729 B1).

Claims 23, 26, 27, 34, and 38 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Slemmer, Giniger, and Jansen (US 6,243,450 B1).

Claims 33 and 41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Slemmer, Giniger, and Bahl (US 6,957,276 B1).

Claim Groupings

Because Appellants argue claim 1 as representative of the invention and rely on those arguments in response to the § 103(a) rejections of claims 23, 26, 27, 33, 34, 38, and 41, we will decide the appeal on the basis of claim 1. *See* 37 C.F.R. 41.37(c)(1)(vii).

PRINCIPLES OF LAW

Claim Interpretation

The *claims* measure the invention. *See SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). During prosecution before the USPTO, claims are to be given their broadest reasonable interpretation, and the scope of a claim cannot be narrowed by reading disclosed limitations into the claim. *See In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997); *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989); *In re Prater*, 415 F.2d 1393, 1404-05 (CCPA 1969). Our reviewing court has

repeatedly warned against confining the claims to specific embodiments described in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc).

"Giving claims their broadest reasonable construction 'serves the public interest by reducing the possibility that claims, finally allowed, will be given broader scope than is justified.'" *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (quoting *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)). "An essential purpose of patent examination is to fashion claims that are precise, clear, correct, and unambiguous. Only in this way can uncertainties of claim scope be removed, as much as possible, during the administrative process." *Zletz*, 893 F.2d at 322. "Construing claims broadly during prosecution is not unfair to the applicant . . . because the applicant has the opportunity to amend the claims to obtain more precise claim coverage." *American Academy,* 367 F.3d at 1364.

Obviousness

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under § 103." *KSR Int'l Co. v. Teleflex, Inc.,* 550 U.S. 398, 419 (2007). "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* at 416.

ANALYSIS

The Examiner rejects claim 1 on the basis of the teachings of Slemmer and Giniger. Appellants argue in the Appeal Brief that Giniger discloses a conventional virtual private network setup established between a plurality of

"edge devices." According to Appellants, an edge device as taught by Giniger cannot be considered an "untrusted access station" as claimed because, *inter alia*, the edge devices are responsible for authentication and encryption with respect to the data on the virtual private network.

The Examiner responds in the Answer that Slemmer's Forced Proxy Server 130 (Fig. 1) is relied upon as teaching the claimed "untrusted access station," not the edge devices as taught by Giniger. Appellants respond, in turn, in the Reply Brief that the goal of the present invention is to establish a secure tunnel from a user terminal to a trusted network element through an untrusted access station, and Giniger does not teach that the edge devices are untrusted or that the communication between the edge devices is through an untrusted access station.

We have considered all of Appellants' arguments in the briefs but conclude that the arguments are not commensurate with the scope of the claimed subject matter. In particular, instant claim 1 might imply, but does not require, that the "untrusted access station" is involved in the distribution of the session key to the terminal and the trusted network element. Nor does the claim require that the untrusted access station be involved in, or part of, the secure tunnel between the terminal and the trusted network element. The only mention of the "untrusted access station" in claim 1 after the step of sending a user authentication packet from the ISP to the terminal "via said untrusted access station" comes in a "wherein" clause. The clause recites that the secure tunnel emulates a physical link "such that" traffic transmitted between the terminal and the Internet via the trusted network element "is secure from modification or eavesdropping by said untrusted access station." A related but separate "secure tunnel" connection between the terminal and

the trusted network element, as contemplated by the rejection and within the scope of the claim, would certainly be "secure from modification or eavesdropping" by the untrusted access station when the access station is not in the communication path of the secure tunnel.[1]

Appellants do seem to contest the Examiner's findings with respect to Slemmer to the extent that Appellants allege, without elaboration, that "there is no disclosure to [sic] suggestion in Slemmer that the access station is untrusted." Reply Br. 5.

However, Appellants do not point to any particular, limiting definition in the Specification for what constitutes an "untrusted" access station. Nor do Appellants provide any extrinsic evidence of some special art-recognized meaning for the term. In the Brief's Summary of Claimed Subject Matter, Appellants emphasize that the "secret session key" is not known to the untrusted access station. App. Br. 6. In the instant rejection, the Forced Proxy Server (Slemmer Fig. 1) does not receive the generated session key that is distributed to the terminal and the trusted network element. Appellants' bare allegation that Slemmer does not disclose or suggest that the access station is "untrusted" does not persuade us of error in the rejection.

We therefore sustain, for the foregoing reasons, the Examiner's § 103(a) rejections.

---

[1] We observe that the claim 1 preamble recites that the method is for establishing secure communication between the terminal and a trusted network element to the Internet "via" an untrusted access station. However, the "via" of the preamble may be fulfilled by the first step of "establishing an association" and the next two steps of "transmitting" and "sending" "via" the untrusted access station.

DECISION

The rejection of claims 1-22, 24, 25, 28-32, 36, 37, 39, and 40 under 35 U.S.C. § 103(a) as being unpatentable over Slemmer and Giniger is affirmed.

The rejection of claims 23, 26, 27, 34, and 38 under 35 U.S.C. § 103(a) as being unpatentable over Slemmer, Giniger, and Jansen is affirmed.

The rejection of claims 33 and 41 under 35 U.S.C. § 103(a) as being unpatentable over Slemmer, Giniger, and Bahl is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED

pgc